Захватываем роутер: массовый скан и брутфорс SSH

Денис Колисниченко , 05.04.2016 11 комментариев 86,446 Добавить в закладки



Содержание статьи

01. Наша цель — твой роутер
02. Сканируем роутеры
03. Кто брутит?
04. Как защитить роутер?

В отличие от полноценных серверов, где обычно настроены PAM (Pluggable Authentication Modules), которые ограничат доступ к серверу на определенное в конфиге время после нескольких (как правило, трех-пяти) неудачных попыток входа, в роутере Линукс обрезанный. PAM на нем нет, поэтому ничто не мешает его брутить. И эта идея — брут и захват роутеров — сегодня, можно сказать, в тренде!

Наша цель — твой роутер

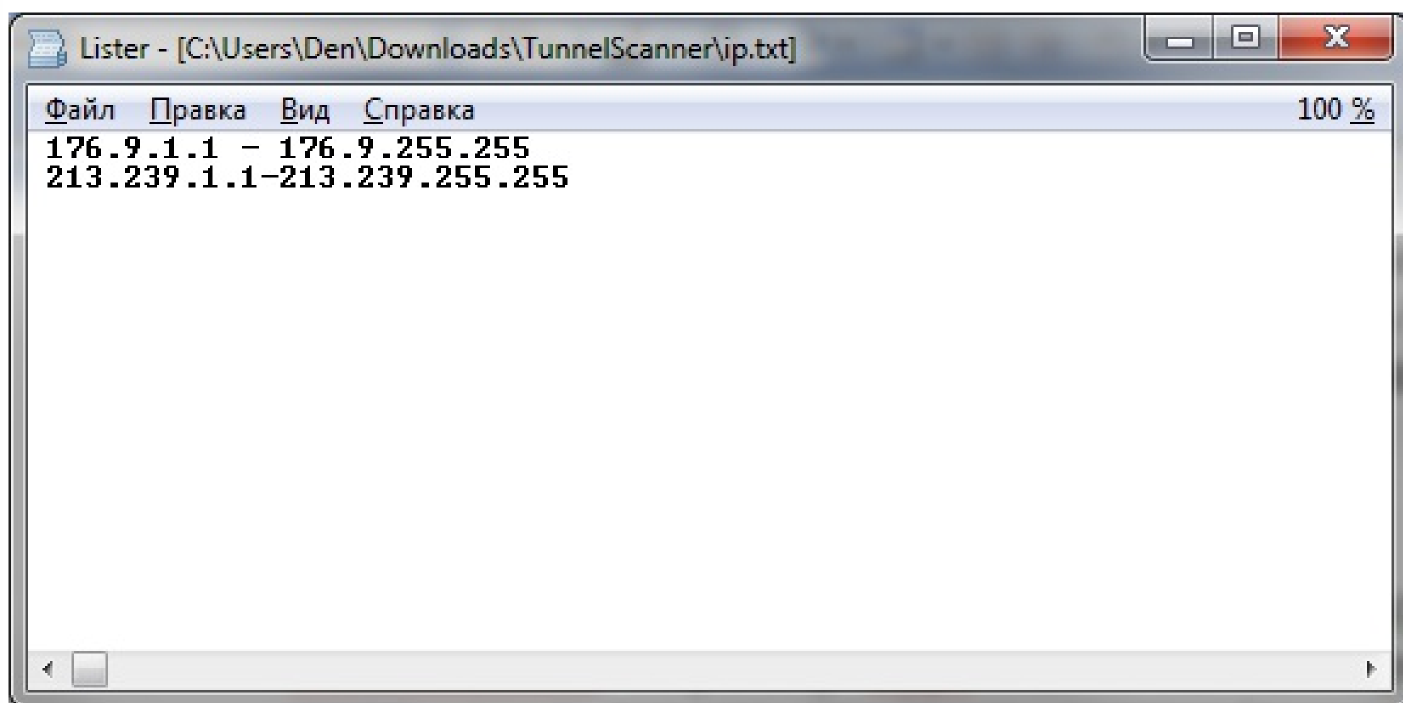
Зачем нужно захватывать роутер? Это зависит от фантазии хакера: можно использовать его для рассылки спама, сделать из него приватный сокс (прокси). А можно продать полученный доступ — стоит это удовольствие, со слов одного моего знакомого, до 200 долларов в месяц, и этот товар пользуется изрядной популярностью.

Сканируем роутеры

Для получения доступа хакеры используют простую, но эффективную программулину Tunnel Scanner. Параметр Type задает тип сканирования: по статическому логину, по статическому паролю, по списку логинов/паролей. Третий вариант (By Login;Password List), как правило, самый эффективный.

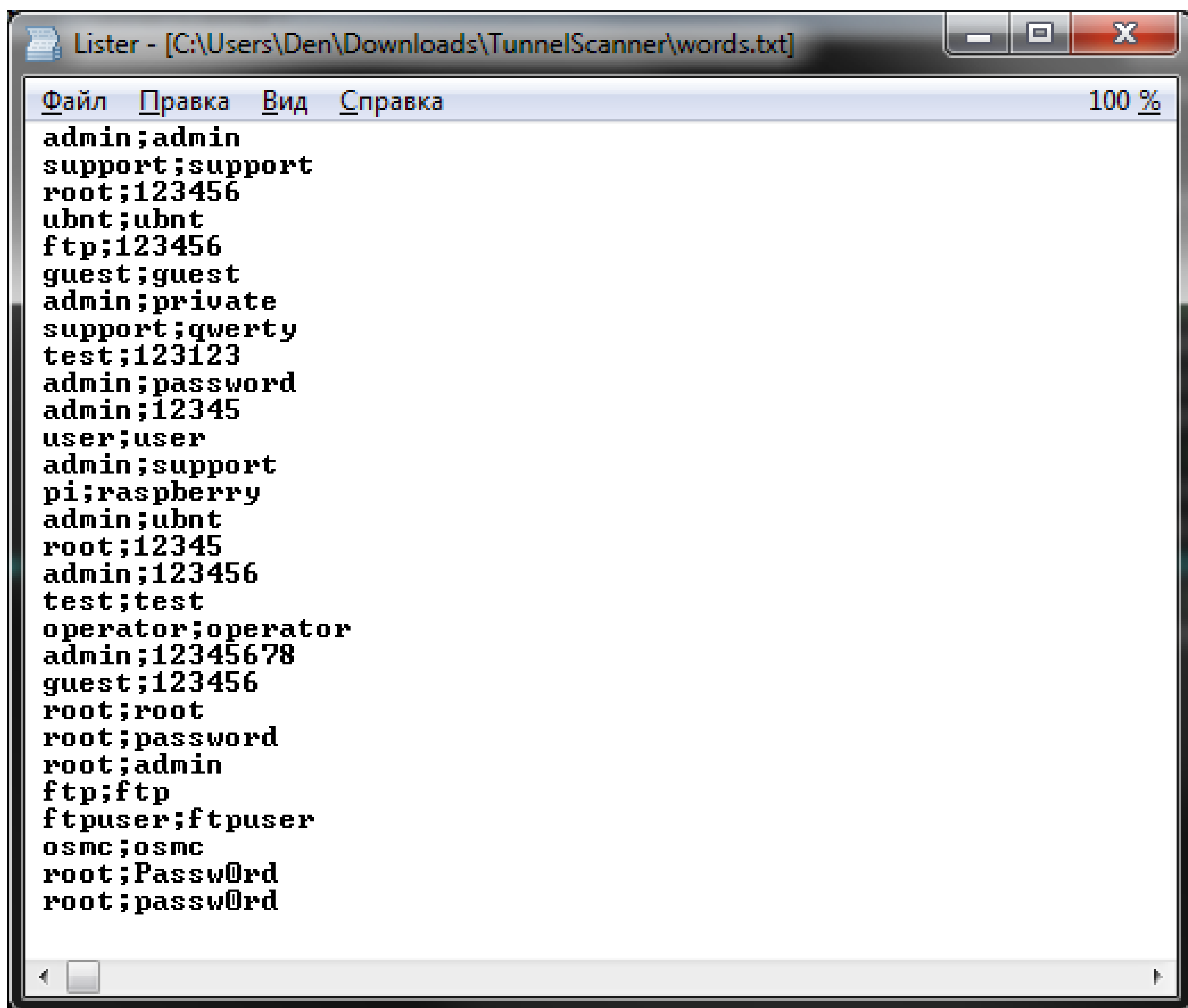
Параметр Static позволяет задать диапазон IP-адресов, который будет сканироваться. Если включить чекбокс IP ranges from file, то

диапазон IP-адресов будет браться из файла, указанного в поле IP ranges (по умолчанию это файл с именем ip.txt). Диапазоны в нем указываются, как показано на скрине ниже.



Файл ip.txt — диапазоны IP-адресов

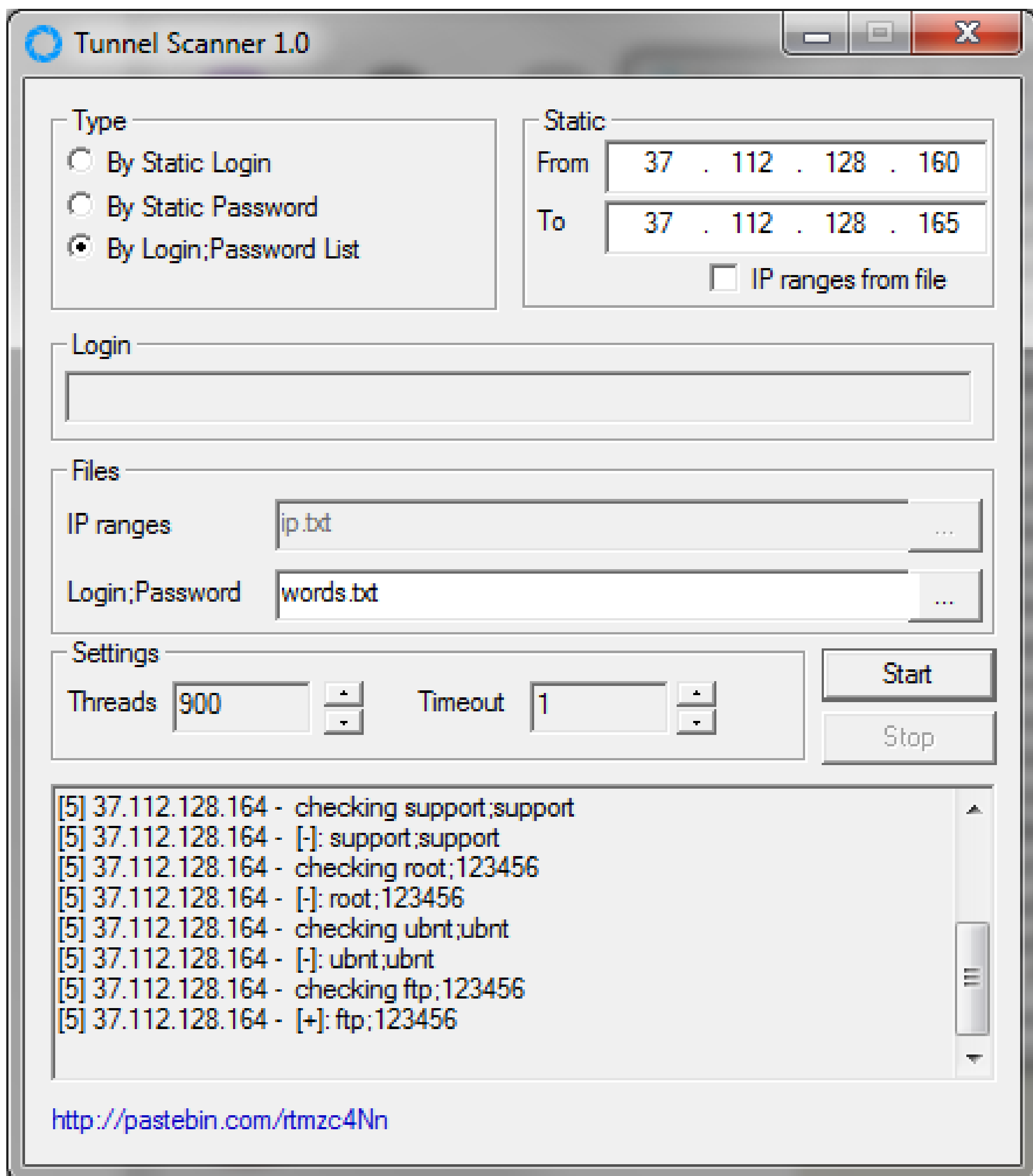
Список логинов и паролей задается параметром Login;Password. По умолчанию он берется из файла words.txt. Конечно, пример списка ниже довольно убогий, но, думаю, в Сети ты без проблем найдешь более продвинутый (или можно проявить смекалку и создать свой).



Список логинов и паролей

Параметр Threads задает количество одновременных потоков для брута. По умолчанию используется значение 900 — этого более чем достаточно. Параметр Timeout определяет тайм-аут в секундах между попытками.

Что ж, осталось нажать кнопку Start.



Программа Tunnel Scanner в работе

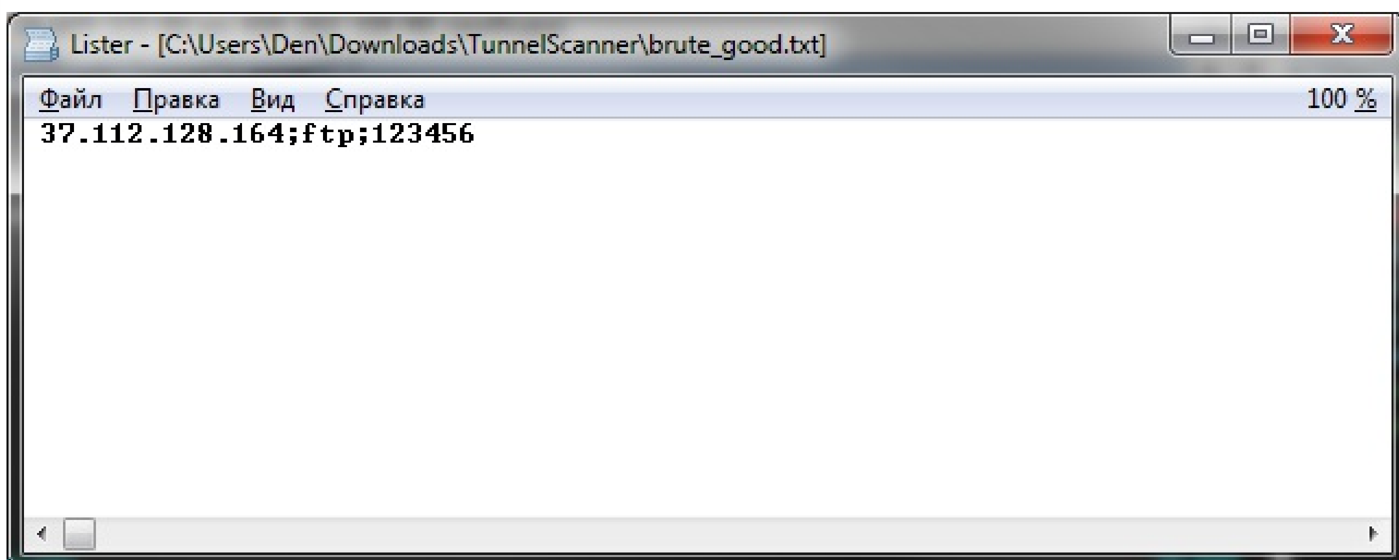
Как видишь, мы уже получили первые результаты. Проанализируем их:

```
[1] 37.112.128.160 -  failed to connect
[5] 37.112.128.164 -  checking admin;admin
[4] 37.112.128.163 -  failed to connect
[3] 37.112.128.162 -  failed to connect
[6] 37.112.128.165 -  failed to connect
[2] 37.112.128.161 -  failed to connect
[5] 37.112.128.164 -  [-]: admin;admin
[5] 37.112.128.164 -  checking support;support
[5] 37.112.128.164 -  [-]: support;support
[5] 37.112.128.164 -  checking root;123456
[5] 37.112.128.164 -  [-]: root;123456
[5] 37.112.128.164 -  checking ubnt;ubnt
[5] 37.112.128.164 -  [-]: ubnt;ubnt
[5] 37.112.128.164 -  checking ftp;123456
[5] 37.112.128.164 -  [+]: ftp;123456
…
```

Номер в квадратных скобках — это номер потока (для нас он не имеет значения). Далее указывается сканируемый IP-адрес. Строка `failed to connect` **означает, что порт SSH закрыт — или совсем, или для нас (брандмауэром). Строка вида** `[-]: admin;admin` **сообщает, что SSH-порт открыт, однако пароль и/или логин не подошел. А вот аналогичная строка с** `+` **говорит, что все удалось:**

```
[5] 37.112.128.164 -  [+]: ftp;123456
```

Это значит, что на машине с IP 37.112.128.164 крутится SSH, войти в систему можно, используя логин ftp и пароль 123456. Результаты последнего удачного сканирования заносятся в файл brute_good.txt. С этим файлом нужно быть очень осторожным — программа перезаписывает его при каждом нажатии кнопки Scan. Поэтому после каждого «улова» нужно делать бэкап этого файла.



Результат удачного сканирования записывается в файл brute_good.txt

Напоследок привожу еще два скрина — сканирование диапазона 37.112.128.100–37.112.128.164. Обрати внимание, на скольких компах в этом диапазоне есть SSH. Сообщений «failed to connect» очень мало.

Tunnel Scanner 1.0

Type
By Static Login
By Static Password
By Login;Password List

Static
From 37 . 112 . 128 . 100
To 37 . 112 . 128 . 164
IP ranges from file

Login

Files
IP ranges ip.txt ...
Login;Password words.txt ...

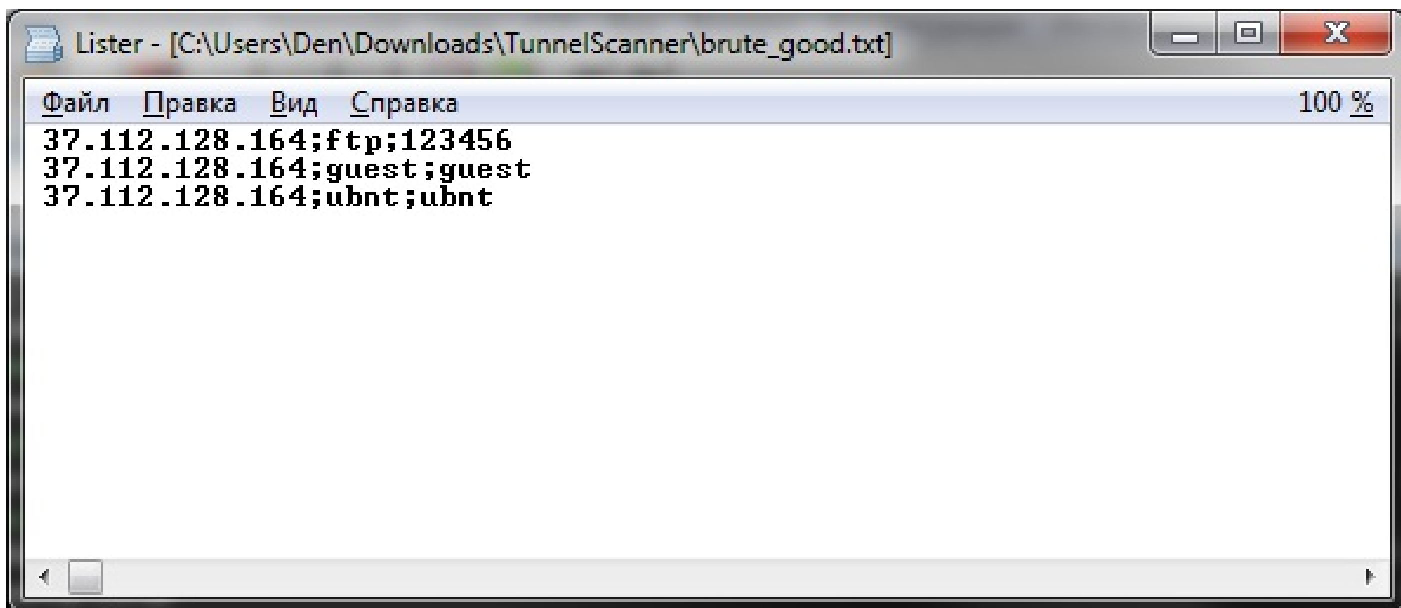
Settings
Threads 900
Timeout 1

Start
Stop

```
[50] 37.112.128.149 - checking ftp;ftp
[31] 37.112.128.130 - [-]: root;admin
[31] 37.112.128.130 - checking ftp;ftp
[50] 37.112.128.149 - [-]: ftp;ftp
[50] 37.112.128.149 - checking ftpuser;ftpuser
[31] 37.112.128.130 - [-]: ftp;ftp
[31] 37.112.128.130 - checking ftpuser;ftpuser
[50] 37.112.128.149 - [-]: ftpuser;ftpuser
[50] 37.112.128.149 - checking osmc;osmc
```

http://pastebin.com/rtmzc4Nn

Сканируем заданный диапазон



«Улов» сканера

Сколько можно так насобирать? Знакомый говорит, что за один день можно получить до 13 000 строк логин/пароль. Это очень много и говорит о том, что даже в наши дни с безопасностью на многих роутерах все запущено.

Кто брутит?

Согласно данным atlas.arbor.net, за последние 24 часа брут SSH был второй по популярности атакой в мире.

TOP ATTACKS (PAST 24 HOURS) GAINERS OVERALL

DESCRIPTION	ATTACKS PER SUBNET	CHANGE FROM YESTERDAY	CVE	PERCENTAGE
VNC network scanning activity	371.34	+22.6 %		65.6%
SSH brute-force login attempts	66.94	+19.9 %		11.8%
ntpdx overflow attempt	44.81	+40.2 %	CVE-2001-0414	7.9%
MYSQL brute-force login attempts	26.48	+41.4 %		4.7%
Outbound Teredo traffic detected	8.79	+57.5 %	CVE-2007-3038	1.6%

[more]

Статистика атак

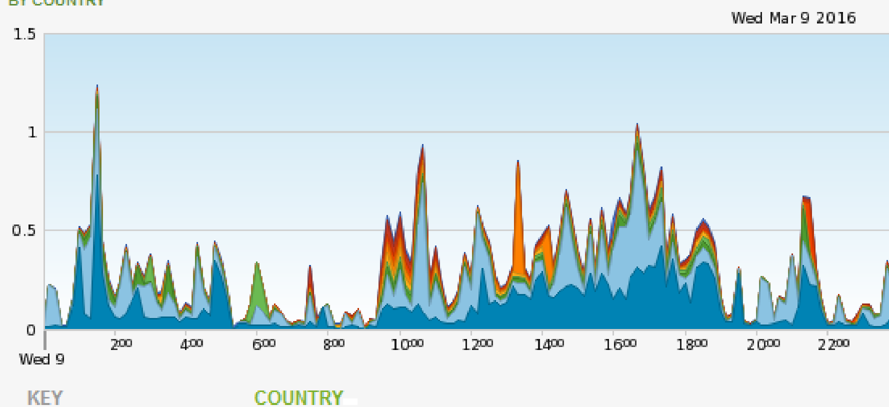
Откуда же исходит угроза? По той же статистике за сутки (сегодня у меня 10 марта 2016 года), чаще всего источник угрозы находится в США, на втором месте — Китай. Конечно, IP-адрес можно изменить, но не думаю, что китайцы особо заморачиваются с этим. Ниже я привел статистику отдельно по всем угрозам и только по SSH-атакам.

TOP THREAT SOURCES (PAST 24 HOURS) HOST ASN COUNTRY

COUNTRY	RANK	ATTACKS PER SUBNET	SCANS PER SUBNET	BOTNETS	PHISHING	DOS
US (United States)	1	94	397.45 kB	3	9260	1567
CN (China)	2	38	557.64 kB	1	318	175
CA (Canada)	3	46	268.25 kB	0	776	34
DE (Germany)	4	8	202.05 kB	1	751	177
KR (South Korea)	5	110	84.32 kB	1	38	624
FR (France)	6	1	80.96 kB	10	643	93
GB (Great Britain)	7	1	44.25 kB	1	1329	127
EU (European Union)	8	0	60.60 kB	0	739	93
PL (Poland)	9	106	48.93 kB	0	257	25
RU (Russian Federation)	10	1	48.72 kB	0	216	84
IN (India)	11	0	14.22 kB	0	286	559
NL (Netherlands)	12	15	32.63 kB	2	337	211
BR (Brazil)	13	0	21.24 kB	0	454	300
TR (Turkey)	14	0	34.76 kB	0	405	15
TW (Taiwan)	15	2	36.44 kB	0	0	0
AU (Australia)	16	1	3.34 kB	0	702	107

Источники угроз за сутки (все угрозы)

SOURCES (PAST 24 HOURS)



KEY	COUNTRY	ATTACKS PER SUBNET	PERCENTAGE
	US (United States)	15.73	23.5%
	CN (China)	15.28	22.8%
	DE (Germany)	2.60	3.9%
	NL (Netherlands)	1.91	2.9%
	FR (France)	1.54	2.3%
	IT (Italy)	1.52	2.3%
	CA (Canada)	1.52	2.3%
	GB (Great Britain)	1.51	2.3%
	UA (Ukraine)	1.09	1.6%
	Other	24.24	36.2%

Источники SSH-атак за сутки

Как защитить роутер?

Есть четыре простых способа:

1. **Роутер настраивается не так часто, и изменять его параметры приходится (после первоначальной настройки) еще реже. Поэтому можно просто отключить SSH. По большому счету он там не особо нужен. Можно включать его только на определенные дни, например когда ты в отпуске и может понадобиться твое вмешательство. Хотя, как правило, роутеры настраиваются по принципу «установил и забыл», но все же.**
2. **Если SSH нужен, тогда следует изменить его порт. Все подобные рассмотренному сканеры проверяют 22-й порт. Они не сканируют все порты узла. Конечно, если захотят пробрутить именно твой роутер, то сканером портов заветный порт будет очень быстро вычислен. Но если нужен любой роутер, то будут сканировать только порт 22.**
3. **Используй сложные пароли. Даже если программа найдет твой SSH-порт, вряд ли она сможет подобрать пароль вроде** `v8KL2BuCLbcySua`.
4. **Настрой брандмауэр так, чтобы доступ к порту SSH разрешался только из определенной подсетки (например, из твоей домашней подсетки — не думаю, что в ней живут миллионы китайцев, желающих пробрутить твой SSH :)).**

Оцени статью:





Денис Колисниченко

Постоянный автор журнала «Хакер»

Теги: SSH Брутфорс Взлом Выбор редактора Статьи